Improving Cybersecurity Skill Development through Visual Programming.

Journal:	*Information and Computer Security*
Manuscript ID	ICS-11-2022-0170
Manuscript Type:	Original Article
Keywords:	Visual Programming Language, Cybersecurity Training, Cyber Range
Note: The following files were submitted by the author for peer review, but cannot be converted to PDF. You must view these files (e.g. movies) online.	
VisualProgramming_Extended.tex	

Improving Cybersecurity Skill Development through Visual Programming

Magdalena Glas[1 [0000−0003−0239−7526]], Manfred Vielberth[1 [0000−0002−1119−4715]], Tobias Reittinger[1 [0000−0001−7458−9928]], Fabian Böhm[1 [0000−0002−0023−6051]], and Günther Pernul[1 [0000−0003−1338−9003]]

University of Regensburg, Universitätsstr. 31, 93053 Regensburg
{firstname.lastname}@ur.de
https://go.ur.de/ifs

Abstract

Purpose – Cybersecurity training plays a decisive role in overcoming the global shortage of cybersecurity experts and the risks this shortage poses to organizations' assets. Seeking to make the training of those experts as efficacious and efficient as possible, we investigate the potential of visual programming languages (VPLs) for training in cyber ranges. For this matter, we integrated the VPL Blockly into an existing cyber range training aiming to facilitate learning a code-based cybersecurity task, namely creating code-based correlation rules for a Security Information and Event Management (SIEM) system.

Methodology – To evaluate the VPL's effect on the cyber range training, we conducted a user study as a randomized controlled trial with 30 participants. In this study, we compared skill development of participants creating SIEM rules using Blockly (experimental group) with participants using a textual programming approach (control group) to create the rules.

Findings – Our study indicates that using a VPL in a cybersecurity training can improve the participants' perceived learning experience compared to the control group while providing equally good learning outcomes.

Originality – The originality of this work lies in studying the effect of using a VPL to learn a code-based cybersecurity task. Investigating this effect in comparison with the conventional textual syntax through a randomized controlled trial has – to the best of our knowledge – not been investigated yet.

Keywords – Visual Programming Language, Cybersecurity Training, Cyber Range

Paper Type – Research paper

1 Introduction

A strong organizational security workforce is essential to address emerging cybersecurity risks and, thus, protect an organization's assets [Furnell et al., 2017]. As the demand for security experts continues to grow, organizations face problems in finding enough sufficiently skilled experts to fill these positions. This workforce shortage is frequently mentioned as the number one barrier to meeting organizational cybersecurity needs [ISC², 2021, Crowley and Filkins, 2022].

According to a recent study by ISC^2 [ISC², 2021] 60% of the study's participants reported that a lack of security experts puts their organizations at risk. The study estimates this skill gap at 3 million unfilled positions worldwide. Investing in organizational cybersecurity training is one approach to overcoming this problem [Pawlicka et al., 2022, Hwang and Helser, 2022]. As conventional training methods like lectures or static e-learning have shown not to be sufficient in transferring practical cybersecurity skills [Crumpler and Lewis, 2019], training in cyber ranges has gained popularity in recent years [Yamin et al., 2020]. Cyber ranges are digital environments that enable hands-on cybersecurity training in a highly realistic infrastructure [National Initiative for Cybersecurity Education (NICE), 2020]. While this approach holds great promise, cyber ranges that are customized to an organization's architecture and infrastructure are a costly and time-consuming endeavor [Vykopal et al., 2017, Nakata and Otsuka, 2021]. For this reason, it is crucial not only to define the learning content conveyed in the process but to examine how training can be designed to be as efficacious and efficient as possible.

Visual programming languages (VPLs) enable users to program with reusable graphical elements instead of writing text-based code [Tsai, 2019]. VPLs are largely used in computer science education to reduce the often-complex syntax of a textual programming language and, thus, facilitate the novices to solve computational problems. In essence, VPLs aim to help learners focus on *what* they want to express, not *how* they do it. Studies in the field demonstrate that students using a VPL achieve better results, show more interest in the topic and find the process more engaging compared to those using a textual programming language [Lye and Koh, 2014, Ouahbi et al., 2015]. In organizational cybersecurity, a plethora of tasks require the use of text-based commands or programs, such as for configuring security systems or using command-line security tools [Newhouse et al., 2017]. Pursuing to facilitate the teaching of these code-based skills in the training of (future) security experts, we address the following research question:

RQ. *Can a VPL support trainees in developing code-based cybersecurity skills?*

In detail, we investigate if using a VPL can make cybersecurity training in a cyber range more efficacious and efficient. We define efficacy as the learning outcome and the learning experience in the learning process. The efficiency of the cyber range training is to be improved by shortening the duration of the training - while retaining its learning content. We tackle the research question by examining the learning process of a particular skill in a Security Operations Center (SOC), namely code-based rule creation for a Security Information and Event Management (SIEM) system. As a foundation, we utilize a cyber range training proposed by [Vielberth et al., 2021], which aims to educate security analysts to learn to create JSON-based SIEM rules. We implement an extension of this concept allowing trainees to create SIEM rules using the VPL Blockly[1]. To investigate whether learners benefit from this approach, we conduct a randomized controlled trial with an experimental group using the novel VPL approach to creating the SIEM rules and a control group using the code-based approach as in the initial work. With this user study, we evaluate the following hypotheses:

H1. *Trainees achieve better learning outcomes when using a VPL.*
H2. *Trainees find training more engaging and less stressful when using a VPL.*
H3. *Trainees learn faster when using a VPL.*

[1] `https://developers.com/blockly`

This work represents an extension of the research we presented at the International Symposium on Human Aspects of Information Security and Assurance 2022 and which is published in the corresponding proceedings [Glas et al., 2022]. The extension of this work allowed us to conduct a more in-depth analysis of the data collected in the user study providing more detailed insight into the impact of a VPL on the participants' learning process (rf. Section 5). In addition, we were able to draw conclusions from the results of the user study as to how the integration of a VPL into a cybersecurity training course can be further improved. Based on these considerations, we improved the extant implementation of the prototypical integration of the VPL as described in Section 6.

The remainder of this work is structured as follows. Section 2 gives an overview of the theoretical background of this research, while Section 3 briefly discusses related work. In Section 4, we introduce our concept of integrating a VPL into cyber range training. Subsequently, Section 5 presents and discusses the evaluation results of the concept's prototypical implementation in the form of a user study. In Section 6 we present a refinement of the implementation based on the findings of the user study. Finally, Section 7 concludes this work and gives an outlook on future research.

2 Background

2.1 Security Operations Center (SOC)

A SOC is the central unit in an organization's cybersecurity. It aims to enhance the organization's overall security posture by identifying security threats, taking appropriate measures, and contributing to regulatory compliance [Vielberth et al., 2020]. A SOC is not a single entity but a complex structure of skilled people working in predefined processes supported by sophisticated tools [Schinagl et al., 2015]. Thus, besides suitable technologies and processes, people are of central importance for successful SOCs [Vielberth et al., 2020], making SOCs dependent on a sufficient number of well-trained security experts. Therefore, it is not surprising that SOCs suffer from the aforementioned skill gap making staffing one of the main challenges modern SOCs are facing [Crowley and Filkins, 2022].

2.2 Security Information and Event Management (SIEM)

A SIEM system is the key technology in a SOC correlating security-relevant events from various sources across an organization [Bhatt et al., 2014]. Incoming security events are correlated by rules created by security experts within the SOC to detect incidents or at least anomalies. These rules are usually created with domain-specific languages, depending on the specific SIEM system. Thus, not only security-related expert knowledge is required to create the rules, but also skills regarding the syntax and semantics of the respective languages. This provides a promising opportunity for cyber range-based training, which can be tailored to the specific corporate infrastructure and the SIEM system in use.

2.3 Cybersecurity Training in Cyber Ranges

The National Institute of Standards and Technology (NIST) defines cyber ranges as "interactive, simulated platforms and representations of networks, systems, tools, and applications" [National Initiative for Cybersecurity Education (NICE), 2020] that provide a safe and legal environment for cybersecurity training, testing, and research. The idea was fed into the field of cybersecurity from the military sector leveraging the concept of a shooting range in which trainees can train their shooting skills in a safe environment [Davis and Magrath, 2013]. Thus, a cyber range allows trainees to learn and practice offensive and defensive cybersecurity skills in a training environment closely resembling a real-world digital infrastructure, such as that of a specific organization. The infrastructures replicated in cyber ranges are not limited to information technology (IT) but can also include operational technology (OT), then referred to as cyber-physical range [Kavallieratos et al., 2019]. Cyber ranges with a training purpose usually include a Learning Management System (LMS) that guides the trainees through a training scenario [Yamin et al., 2020]. Typically, a LMS comprises learning material in the form of videos and texts as well as tasks for the trainee to solve during the training, often enhanced with gamification aspects such as a scoring system.

3 Related Work

[Böhm et al., 2022] propose to use a VPL to simplify cybersecurity tasks that require a high amount of operational knowledge, such as the syntax of a specific security analytics tool. For this matter, the authors present a prototype that integrates a VPL into the productive security operations of an organization. Abstracting code-based security tasks entirely through a VPL can be a laborious undertaking. Additionally, it may not be possible to map the full functional scope of a tool by a VPL integration. This means that not every task that a security expert needs to master can be abstracted through a VPL or that this might not always be appropriate. Instead, we see the potential of a VPL in facilitating knowledge transfer and suggest to use a VPL to facilitate learning a code-based task, not modifying the task itself.

In the context of teaching and training, VPLs are commonly used to teach basic programming concepts to first-time coders. In a study by Tsai [Tsai, 2019], for example, participants were taught programming concepts over several weeks. During this time, the experimental group attended a class in which a VPL was used. The control group attended a conventional computer science class. This study shows that those participants learning with the VPL outperformed the control group. Beyond that, VPLs can facilitate learners to gain domain-specific knowledge that requires programming to some extent. The works investigating this matter do not use VPLs for teaching programming skills but for a simpler, better-understandable representation of the source code. [Rao et al., 2018] present a VPL-based learning environment for data science and machine learning. The platform is built for learners to understand and apply complex computer-assisted analyses, despite having little programming experience. [Lédeczi et al., 2019] use a VPL in a networked robotics environment to introduce learners to networking aspects of cybersecurity. The latter two studies, however, focus on the overall learning environment rather than the specific impact of the VPL on the learning process. This paper aims to apply a VPL to transfer skills and knowledge in cybersecurity to investigate the specific impact of using the VPL on the learning process. For this reason, we perform a comprehensive user study following a two-group experimental design (randomized controlled trial) similar to the previously mentioned study by Tsai [Tsai, 2019]. This has – to the best of our knowledge – not been attempted in the field of cybersecurity learning yet.

4 Integrating a VPL into Cyber Range Training

We integrate a VPL into an existing cyber range concept proposed by [Vielberth et al., 2021] to investigate the potential of VPLs in cybersecurity training. What follows is a short description of this underlying concept before we outline the integration of the VPL approach.

4.1 Cyber Range Concept

The cyber range concept by [Vielberth et al., 2021] aims to train future SOC analysts in configuring a SIEM system. The virtual environment of the training is a digital twin-based simulation of an industrial control system (ICS) against which a simulated attacker performs various attacks. The simulated ICS produces real-time log data that is transferred to a SIEM system. Thereby, each log entry is interpreted as a security event. The trainees take on the role of SOC analysts monitoring the ICS, detecting the attacks, and configuring the SIEM system for automatic attack detection. They interact with the cyber range over a web-based frontend consisting of the UI of the SIEM system and a LMS, which provides them information about the ICS scenario, theoretical background on SIEM rule definition and includes the five overall tasks trainees solve throughout the training. Each task addresses a specific attack against the ICS, which the trainees first manually investigate by analyzing the incoming security events in the SIEM system. Building on this, they define a SIEM rule that automatically detects when the event or sequence of events indicating the attack appears in the SIEM system to trigger a SIEM alarm automatically. As an example, the SIEM rule "Unknown IP in network" (Task 1), which is shown in Figure 2, triggers an alarm for every incoming security event "FIREWALL WARNING". As illustrated in Figure 1 the trainees create increasingly complex rules in two different task types. In Tasks 1, 2, and 3, large parts of the rule are given and the trainees only fill out missing gaps (*Cloze Task*, rf. Figure 2). In Tasks 4 and 5, the trainees create entire rules themselves, only using a text editor to create the rules in actual JSON (*Editor Task*, rf. Figure 3).

For a deeper insight into the cyber range scenario and technical implementation of the prototype, please refer to the original work [Vielberth et al., 2021]. Based on this concept, we want to investigate whether trainees can learn better to create code-based SIEM rules when using a VPL. The integration of this approach in the existing cyber range is described in the following subsection.

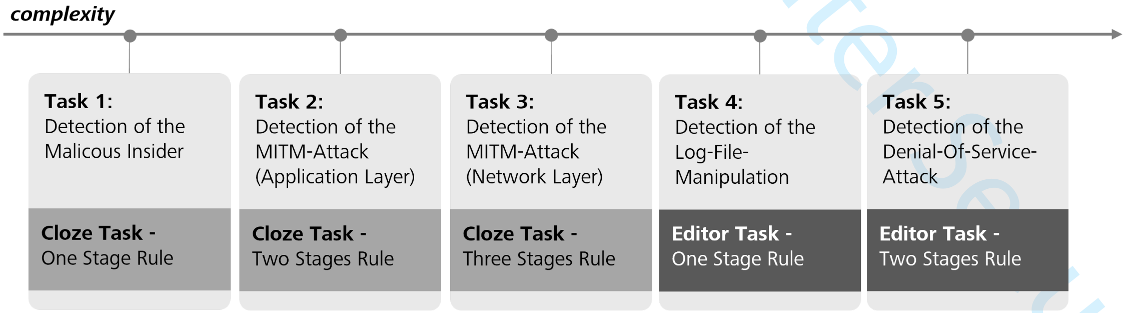
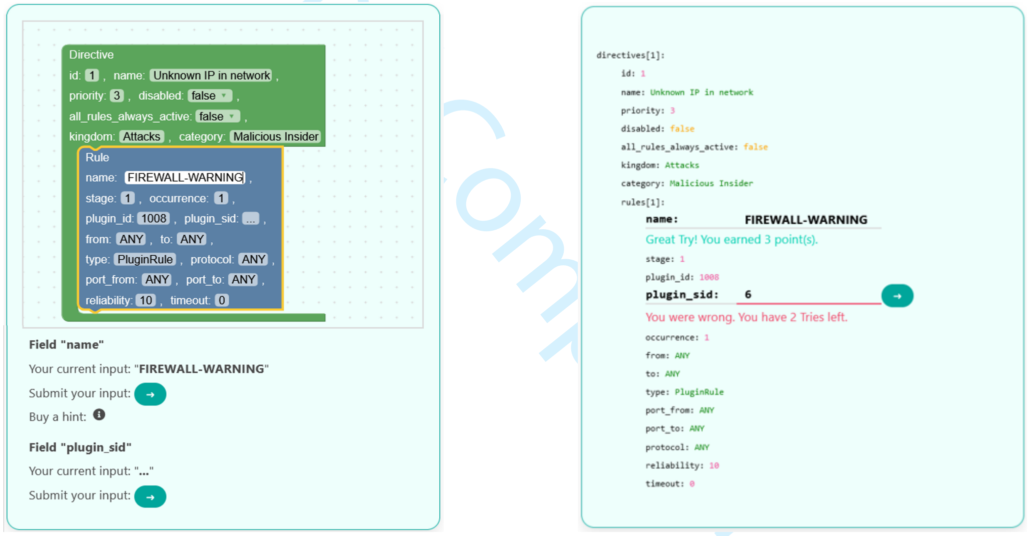

complexity
Task 1:
Detection of the Malicous Insider
Cloze Task -
One Stage Rule
Task 2:
Detection of the MITM-Attack (Application Layer)
Cloze Task -
Two Stages Rule
Task 3:
Detection of the MITM-Attack (Network Layer)
Cloze Task -
Three Stages Rule
Task 4:
Detection of the Log-File-Manipulation
Editor Task -
One Stage Rule
Task 5:
Detection of the Denial-Of-Service-Attack
Editor Task -
Two Stages Rule

Figure 1. Sequence of tasks in the cyber range training.

4.2 SIEM Rule Creation with Blockly

For our study, we seek to integrate a VPL in the the original cyber range concept. As a VPL, we use the open-source library Blockly, which fulfills essential requirements to successfully integrate it into the cyber range proposed by [Vielberth et al., 2021]. First, it is web-based and, therefore, can be directly used within the existing frontend. Additionally, Blockly is highly dynamic and allows the creation of custom blocks, which is necessary to map the domain-specific language of the SIEM system Dsiem[2] used within the cyber range.

Blockly leverages graphical blocks to display concepts of the underlying domain-specific language (e.g., a programming language or a language to describe SIEM rules) without knowing the syntax of this language. With the Blockfactory[3], Blockly offers a simple way to define custom blocks for a specific language. Figures 2a and 3a illustrate the two custom blocks we defined for the integration into the cyber range: the green *header* block and the blue *rule* block. Comparing this Blockly-based rule with the JSON-based description of the same rule (Figure 3b) highlights that Blockly allows for a more compact representation and does not contain syntax-specific elements such as braces or quotation marks. The full integration is publicly available on GitHub[4].



Directive
id: 1 , name: Unknown IP in network ,
priority: 3 , disabled: false ▾ ,
all_rules_always_active: false ▾ ,
kingdom: Attacks , category: Malicious Insider
Rule
name: FIREWALL-WARNING ,
stage: 1 , occurrence: 1 ,
plugin_id: 1008 , plugin_sid: ... ,
from: ANY , to: ANY ,
type: PluginRule , protocol: ANY ,
port_from: ANY , port_to: ANY ,
reliability: 10 , timeout: 0

Field "name"

Your current input: "**FIREWALL-WARNING**"

Submit your input: →

Buy a hint: ℹ

Field "plugin_sid"

Your current input: "**...**"

Submit your input: →

(a) Blockly mode.

```
directives[1]:
    id: 1
    name: Unknown IP in network
    priority: 3
    disabled: false
    all_rules_always_active: false
    kingdom: Attacks
    category: Malicious Insider
    rules[1]:
        name:            FIREWALL-WARNING
        Great Try! You earned 3 point(s).
        stage: 1
        plugin_id: 1008
        plugin_sid:    6                 →
        You were wrong. You have 2 Tries left.
        occurrence: 1
        from: ANY
        to: ANY
        type: PluginRule
        port_from: ANY
        port_to: ANY
        protocol: ANY
        reliability: 10
        timeout: 0
```

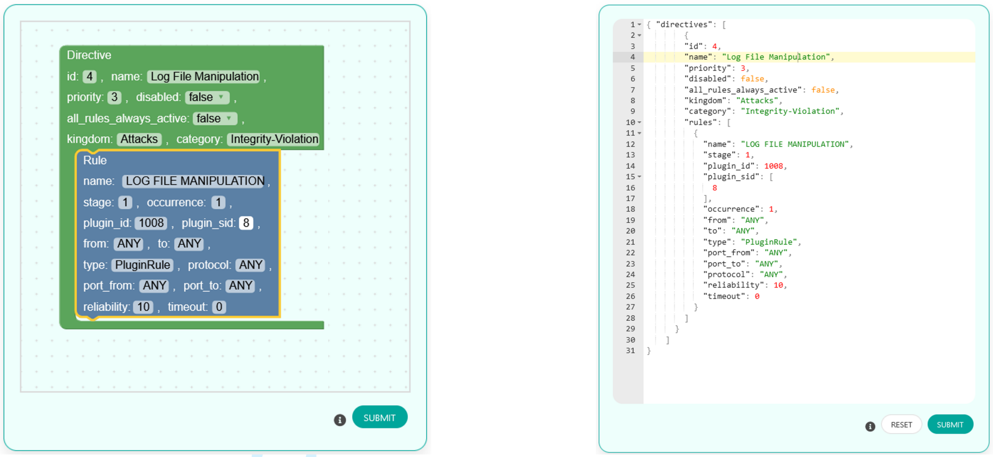
(b) JSON mode.

Figure 2. Comparison of a *Cloze Task* (Task 1) in Blocky and JSON mode.

[2] https://www.dsiem.org/

[3] https://blockly-demo.appspot.com/static/demos/blockfactory/index.html

[4] https://github.com/BlocklyCyberRange



```
Directive
id: 4 , name: Log File Manipulation ,
priority: 3 , disabled: false ▾ ,
all_rules_always_active: false ▾ ,
kingdom: Attacks , category: Integrity-Violation
  Rule
  name: LOG FILE MANIPULATION ,
  stage: 1 , occurrence: 1 ,
  plugin_id: 1008 , plugin_sid: 8 ,
  from: ANY , to: ANY ,
  type: PluginRule , protocol: ANY ,
  port_from: ANY , port_to: ANY ,
  reliability: 10 , timeout: 0
```

```
{ "directives": [
    {
    "id": 4,
    "name": "Log File Manipulation",
    "priority": 3,
    "disabled": false,
    "all_rules_always_active": false,
    "kingdom": "Attacks",
    "category": "Integrity-Violation",
    "rules": [
      {
        "name": "LOG FILE MANIPULATION",
        "stage": 1,
        "plugin_id": 1008,
        "plugin_sid": [
          8
        ],
        "occurrence": 1,
        "from": "ANY",
        "to": "ANY",
        "type": "PluginRule",
        "port_from": "ANY",
        "port_to": "ANY",
        "protocol": "ANY",
        "reliability": 10,
        "timeout": 0
      }
    ]
  }
 ]
}
```

(a) Blockly mode.

(b) JSON mode.

Figure 3. Comparison of an *Editor Task* (Task 5) in Blocky and JSON mode.

5 Evaluation

To evaluate the impact of the VPL on the cyber range training, we conducted a user study based on three hypotheses regarding the improvement of learning outcome (**H1**), learning experience (**H2**), and efficiency (**H3**) of the training.

H1. *Trainees achieve better learning outcomes when using a VPL.*
H2. *Trainees find training more engaging and less stressful when using a VPL.*
H3. *Trainees learn faster when using a VPL.*

Hereafter, we describe the method and procedure we followed for the user study before presenting the study results. For transparency and reproducibility, the complete data set, the SPSS analysis outputs, and all questionnaires and surveys of the user study are published on GitHub[5].

5.1 Method & Procedure

To test the hypotheses, we conducted a randomized controlled trial [Torgerson and Torgerson, 2001]. Participants of each group had to complete the full cyber range training creating SIEM rules in both task modes (*Cloze Task* and *Editor Task*) as described in Section 4.1. While the experimental group ($n = 15$) used Blockly to create the SIEM rules, the control group ($n = 15$) created the rules in the original JSON syntax. As intended by the randomized controlled trial experiment design, participants were randomly assigned to one of the two groups prior to training. The study participants were students recruited from undergraduate and graduate cybersecurity classes within business informatics curricula at a German university. Out of the 30 participants, eight identified as female, and 22 identified as male. The study was conducted in January 2022. As personal contact was supposed to be kept to a minimum at this time due to

[5] `https://github.com/BlocklyCyberRange/userStudy`

COVID-19 restrictions, the participants took part in the training remotely. For this matter, we set up a video conference session to welcome the participants and explain the training procedure. The evaluation procedure is illustrated in Figure 4 and described in detail hereafter.

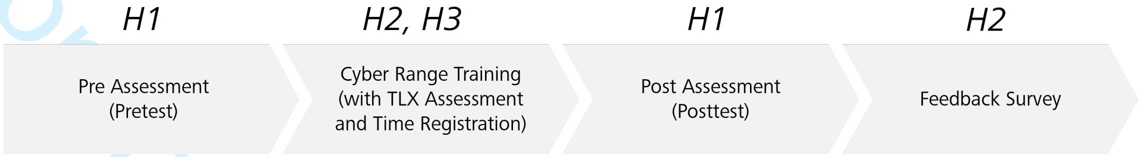

H1
Pre Assessment (Pretest)
H2, H3
Cyber Range Training (with TLX Assessment and Time Registration)
H1
Post Assessment (Posttest)
H2
Feedback Survey

Figure 4. Procedure of the evaluation.

H1: Learning Outcome. To measure the learning outcome in both groups, we chose a pre-test/post-test design assessing the participants' skills and knowledge before and after the training. The assessment was conducted with a multiple-choice quiz assessing skills and knowledge in four categories:

- Non-security-related knowledge
- Attack-related knowledge
- SIEM-related knowledge
- SIEM rule-related skills

Each category was assessed with three items resulting in a questionnaire containing twelve items. We define the difference in the mean value of correctly answered tasks per category before and after training as learning outcome. This learning outcome was assessed for each participant to then compare the learning outcomes of the two groups.

H2: Learning Experience. To evaluate H2, we measured both the participants' perceived workload during the training and their overall engagement in the training. As outlined in Subsection 4.1, the cyber range training entails tasks of increasing difficulty in two different task types. Assessing the participants' perceived workload after completing each of these tasks makes it possible to precisely distinguish at which stages of the training the VPL improved the participants' learning experience and where it did not. For this matter, we utilized the NASA Task Load Index (TLX) [Hart and Staveland, 1988]. The TLX was initially designed to measure the perceived workload for operators interacting with a human-machine interface. The scale consists of six subscales representing sources of workload: *Mental Demand (MD)*, *Physical Demand (PD)*, *Temporal Demand (TD)*, *Performance (PE)*, *Effort (EF)*, and *Frustration Level (FL)*. A task is rated by assigning it a value on each subscale. These values are then combined to determine the workload of the task. Today, the TLX is considered a common method for workload assessment in various application areas [Hart, 2006]. In this regard, the TLX can also be utilized to capture purely cognitive workload, e.g., to evaluate the usability of web applications [Schmutz et al., 2009]. To assess the cognitive workload for the tasks of the cyber range training, we exclude the subscales *Physical Demand* and *Effort*. The former because the training does not include any physical aspects, the latter because – in our case – this subscale is equivalent to *Mental Demand*. This results in a set of four TLX-specific questions, one for each remaining subscale (rf. Table I).

To simplify the scoring for participants, we chose a Likert scale from 1 to 5 (*low* to *high* for MD, TD, and FL, respectively, *good* to *poor* for PE) instead of the original TLX scale from 1 to 100. We integrate a TLX module in the LMS of the existing cyber range. The TLX module appears every time a participant completes a task.

ID	Description
MD	How mentally demanding was the task?
TD	How hurried or rushed was the pace of the task?
PE	How successful were you in accomplishing what you were asked to do?
FL	How insecure, discouraged, irritated, stressed, or annoyed were you?

Table I. TLX-based items to assess the perceived workload of each task of the cyber range training (to be rated on a Likert scale from 1 to 5 – *low* to *high* for MD, TD, and FL and *good* to *poor* for PE, respectively).

To assess the participants' overall engagement in the training, we designed a post-training feedback survey based on the ARCS model for learning motivation by Keller [Keller, 1987]. The model presumes that intrinsic motivation can be achieved when a learning process meets the four conditions *Attention*, *Relevance*, *Confidence*, and *Satisfaction*. The subjective perception of whether a learning process was successful is another relevant factor contributing to the intrinsic motivation to learn [Efklides, 2011]. Thus, we complemented the four ARCS conditions with a fifth condition: *Metacognition*. Each condition is measured with two items in the form of statements, to which the participants rate their level of agreement on a Likert scale from 1 (fully disagree) to 5 (fully agree). As an example, the two items measuring the condition *Attention* are shown in Table II.

ID	Description
A1	The scenario and context of the training were interesting.
A2	I wanted to successfully finish the training and complete all the tasks.

Table II. Items *A1* and *A2* assessing the condition *Attention* (to be rated on a Likert scale from 1 to 5 – *fully disagree* to *fully agree*).

H3: Learning Efficiency. To measure the efficiency of the VPL used in the cyber range training (H3), we recorded the timestamp at the beginning of the training and whenever a participant started and completed a task during the training. This allows for determining how long it takes a participant to complete each task.

5.2 Results & Discussion

In this section, we present and discuss the user study results with regard to the three hypotheses.

H1: Learning Outcome. We performed a paired t-test across all knowledge categories to investigate learning efficacy, comparing the mean rate of correctly answered questions for each category and overall in pre- and post-test. As shown in Table III and depicted in Figure 5, the mean rate of correctly answered questions improved in every category and overall for both groups. The results were significant in the categories *Attack-related knowledge*, *SIEM rule-related skills* and across all categories (*Overall*) in both groups. A significant increase in *Non-security-related knowledge* could be observed only for the control group.

Group	Category	M (Pre)	SD (Pre)	M (Post)	SD (Post)	t	df	Sig (2-tailed)
Blockly	Non-sec.-related	.64	.29	.80	0.21	-1.83	14	.089
	Attack-related	.80	.17	.93	.14	-3.06	14	.009
	SIEM-related	.84	.21	.89	.16	-1.00	14	.334
	SIEM rule-related	.35	.39	.87	.25	-4.08	14	.001
	Overall	.66	.15	.87	.10	-5.43	14	<.001
JSON	Non-sec.-related	.49	.21	.67	0.18	-2.48	14	.027
	Attack-related	.64	.27	.80	.21	-2.17	14	.048
	SIEM-related	.73	.26	.84	.21	-1.43	14	.173
	SIEM rule-related	.22	.21	.76	.29	-6.29	14	<.001
	Overall	.52	.13	.77	.17	-4.61	14	<.001

Table III. Results of learning outcome (H1): Comparison of increase in performance from pre- to post-test in both groups.

To compare the learning outcome between the two groups, we examined the change in their performance, that is, the difference in percentage points of correctly answered questions between pre- and post-test. For this matter, an unpaired t-test was conducted. The results, shown in Table IV show a similar increase in performance in both groups and do not indicate that either JSON or Blockly performed significantly better than the other. In summary, both modalities resulted in similarly good learning outcomes. Even though the total post-test results of the Blockly group were better than those of the control group, the differences in percentage points were similar in both groups. Accordingly, no significant impact of Blockly on the participants' learning outcome could be noted. For this reason, we reject H1.

It should be noted here, however, that prior knowledge was unequal in the two groups, as the Blockly group's pre-test results were consistently better across all categories. The potential for performance improvement in the Blockly group was correspondingly lower, which limits the comparability of the results. For this reason, this aspect should be further investigated in a future study, in which a higher number of participants should ensure better comparability of both groups.

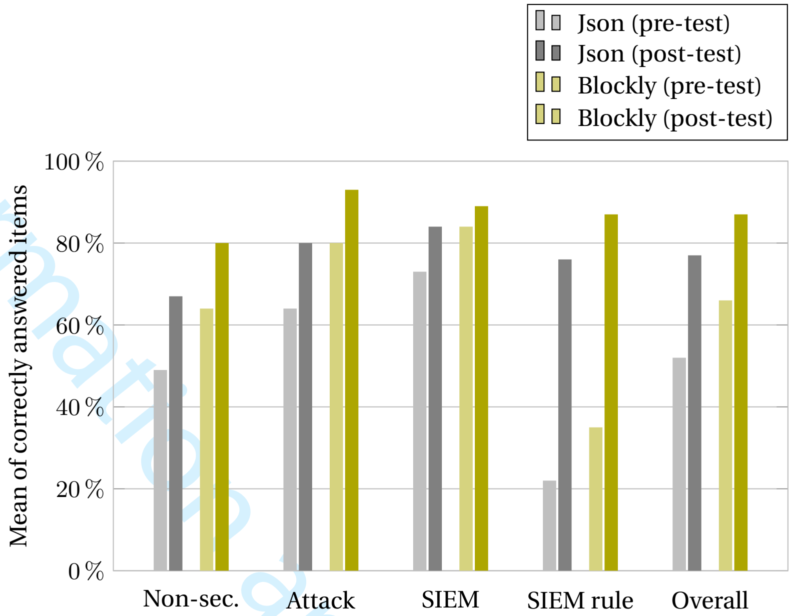


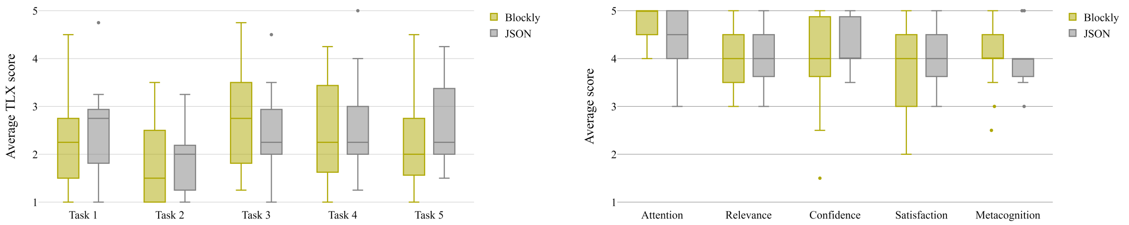
Figure 5. Graphical representation of learning outcome in both groups.

Category	**M (Blockly)**	**SD (Blockly)**	**M (JSON)**	**SD (JSON)**	**t**	**df**	**Sig (2-tailed)**
Non-sec.-related	.16	.33	.18	.28	-.20	27.21	.843
Attack-related	.13	.17	.16	.28	.27	23.11	.794
SIEM-related	.04	.17	.11	.30	-.75	22.32	.463
SIEM rule-related	.51	.49	.53	.33	-.15	24.59	.885
Overall	.21	.15	.24	.21	-.51	25.69	.616

Table IV. Results of learning outcome (H1): Comparison of the difference in the percentage points of correctly answered questions between pre-and post-test between the two groups.

H2: Learning Experience. For H2, an unpaired t-test was performed to compare the perceived workload in the two groups (cf. Table V and Figure 6a). The mean perceived workload was lower for four of the five tasks in the Blockly group. This difference was particularly noticeable in Task 1 and Task 5, indicating that Blockly's potential is notable especially in unfamiliar tasks (Task 1) and particularly complex tasks (Task 5).

Likewise, an unpaired t-test for the five conditions measuring the participants' learning motivation (ARCSM) was conducted (cf. Table VI and Figure 6b). While the conditions *Confidence* and *Satisfaction* were higher among the control group, *Attention* and *Metacognition* were higher in the Blockly group. The mean rating of *Relevance* was about the same in both groups. A possible explanation for this result is that all participants had some prior experience in textual programming due to their study background. When solving the tasks with Blockly the participants



(a) Perceived workload based on TLX.

(b) Engagement based on ARCSM.

Figure 6. Graphical representation of H2 (learning experience) results.

Task	M (Blockly)	SD (Blockly)	M (JSON)	SD (JSON)	t	df	Sig. (2-tailed)
Task 1	2.25	0.93	2.53	0.90	-0.85	27.97	.404
Task 2	1.78	0.83	1.88	0.68	-0.36	26.98	.721
Task 3	2.67	1.06	2.45	0.91	0.60	27.36	.552
Task 4	2.57	1.06	2.58	0.98	-0.04	27.80	.965
Task 5	2.35	1.01	2.62	0.85	-0.78	27.24	.442

Table V. Results of learning experience (H2): Perceived workload based on TLX.

Condition	M (Blockly)	SD (Blockly)	M (JSON)	SD (JSON)	t	df	Sig (2-tailed)
Attention	4.67	0.41	4.43	0.65	1.18	23.54	.251
Relevance	4.03	0.55	4.07	0.56	-0.16	27.99	.871
Confidence	4.00	0.98	4.30	0.53	-1.04	21.47	.309
Satisfaction	3.67	0.96	4.00	0.57	-1.16	22.74	.258
Metacognition	4.10	0.71	3.97	0.52	.59	25.53	.562

Table VI. Results of Learning Experience (H2): Engagement based on ARCS(M).

had to engage with something new. Thus, the Blockly participants were less satisfied and confident than the JSON participants yet found the learning process more interesting (*Attention*).

These results are consistent with the verbal feedback from participants, in which the Blockly approach was rated very positively overall. For this reason, we conclude that the use of Blockly has the potential to improve the learning experience to some extent. Although this cannot be shown to be significant in our user study, partly because of the relatively small number of participants, we consider the results to be a good indicator and therefore accept H2.

H3: Learning Efficiency. For the third hypothesis, an unpaired t-test was performed to compare the average time it took the participants to solve each task for the two groups (H3). While the control group performed better in Tasks 2, 3 and 4, the Blockly group performed better in Tasks 1 and 5. As the perceived workload (H2) in the Blockly group was also rated lower for these tasks, this observation possibly supports the assumption that Blockly achieves to facilitate solving novel and particularly complex tasks. In general, however, we realized that the time to complete a task is due to more factors than its sheer modality. Participants told us, e.g., that they interrupted the training for short breaks or were facing technical issues such as a weak internet connection. This is visible by the outliers depicted in Figure 7, especially in the Blockly group. Thus, because the data collected are limited in determining whether Blockly improved participants' learning efficiency, we can neither reject nor accept H3.

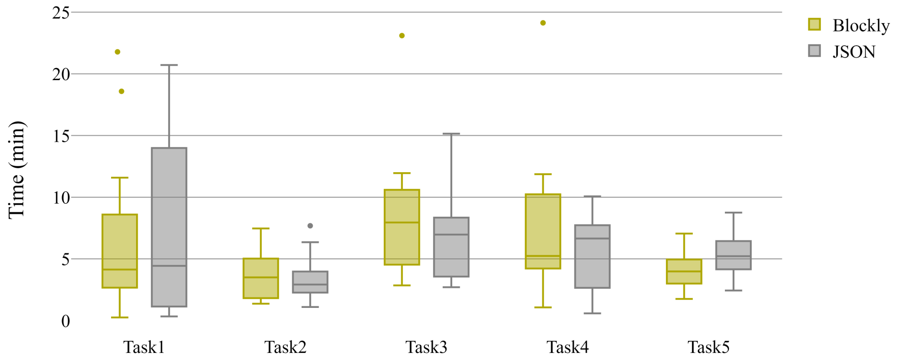


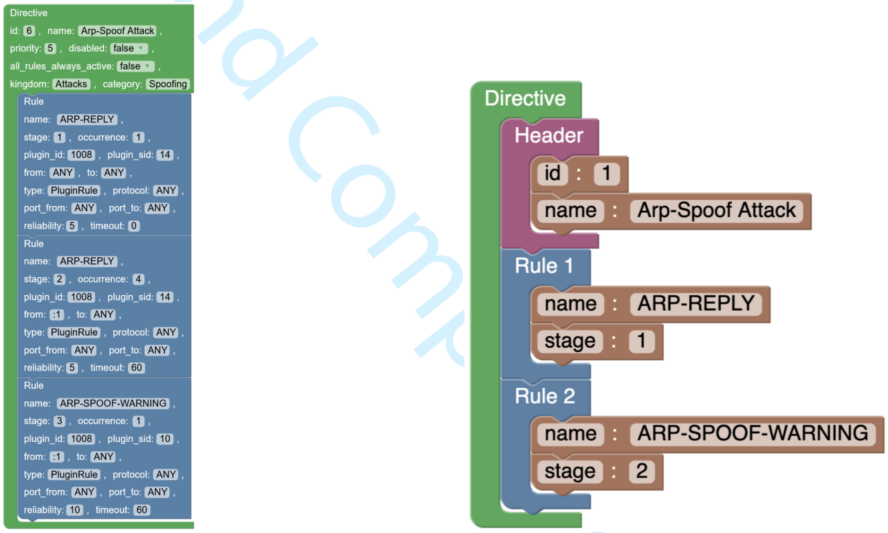
Figure 7. Graphical Representation of Learning Efficiency (H3) results.

Task	M (Blockly)	SD (Blockly)	M (JSON)	SD (JSON)	t	df	Sig (2-tailed)
Task 1	06:38	06:19	07:07	06:53	-.20	27.89	.844
Task 2	03:41	02:12	03:21	01:44	0.45	26.56	.654
Task 3	08:37	04:59	06:39	03:29	1.25	15.07	.223
Task 4	07:27	05:37	05:21	03:12	1.26	22.20	.220
Task 5	04:11	01:25	05:11	01:44	-1.75	26.98	.091

Table VII. Results of Learning Efficiency (H3): Time assessment.

6 Refinement of the VPL Integration

While the participants' verbal feedback regarding the Blockly approach was very positive overall, some noted that the large number of attributes in a SIEM-related Blockly element was overwhelming at first and made it difficult to identify those fields relevant to a specific task. In the extant prototypical implementation, every possible attribute of a SIEM rule is visible. As a result, each attribute cannot be implemented in a single row, as this would take up a large amount of vertical space. Therefore, multiple attributes are aligned into a single row based on their respective text length. This representation of the original JSON syntax might lead to the participants being overwhelmed by the number of different attributes at first. Since only a few fields need to be modified for each task and the majority of the attributes are assigned default values (e.g., plugin_id), the representation of a rule could be further simplified by reducing a block to those attributes that are subject to a particular task. This further abstraction of the original syntax is intended to help trainees grasp the structure and content of a rule more quickly and, thus, counteracts the trainees' initial overwhelm described above. We are aware that this additional abstraction further reduces the complexity of the rules. Thus, the comparability of the refined Blockly integration to the original JSON design in terms of difficulty is limited. This must be taken into account in a future user study.



```
Directive
id: 6 , name: Arp-Spoof Attack ,
priority: 5 , disabled: false ▾ ,
all_rules_always_active: false ▾ ,
kingdom: Attacks , category: Spoofing
  Rule
  name: ARP-REPLY ,
  stage: 1 , occurrence: 1 ,
  plugin_id: 1008 , plugin_sid: 14 ,
  from: ANY , to: ANY ,
  type: PluginRule , protocol: ANY ,
  port_from: ANY , port_to: ANY ,
  reliability: 5 , timeout: 0
  Rule
  name: ARP-REPLY ,
  stage: 2 , occurrence: 4 ,
  plugin_id: 1008 , plugin_sid: 14 ,
  from: :1 , to: ANY ,
  type: PluginRule , protocol: ANY ,
  port_from: ANY , port_to: ANY ,
  reliability: 5 , timeout: 60
  Rule
  name: ARP-SPOOF-WARNING ,
  stage: 3 , occurrence: 1 ,
  plugin_id: 1008 , plugin_sid: 10 ,
  from: :1 , to: ANY ,
  type: PluginRule , protocol: ANY ,
  port_from: ANY , port_to: ANY ,
  reliability: 10 , timeout: 60
```

(a) Extant prototype.

```
Directive
  Header
    id : 1
    name : Arp-Spoof Attack
  Rule 1
    name : ARP-REPLY
    stage : 1
  Rule 2
    name : ARP-SPOOF-WARNING
    stage : 2
```

(b) Refinement prototype.

Figure 8. Comparison of the refinement and the extant prototype.

The refinement is integrated into a new prototype illustrated in Figure 8b. The prototype consists of four different blocks. The green block is a directive block that can contain one header block and multiple rule blocks. Both the magenta-red colored header block and the blue-colored rule block can contain multiple attribute blocks. The brown-colored attribute blocks contain two input fields for the key and value of the attribute. Comparing this refinement with the extant prototypical implementation (Figure 8a) highlights that the optimization allows for an even more compact and clear representation. The four custom blocks are publicly available on GitHub[6] as an export from the Blockfactory.

7 Conclusion

In this work, we integrated a VPL into an existing cyber range training and evaluated its effects on learning outcome, learning experience, and learning efficiency in a randomized controlled trial. The study indicates learning outcomes to be equally good for the experimental group (using the VPL) and the control group (using text-based programming). While a successful learning outcome is considered the primary goal of cyber range training, it is also highly desirable to raise trainees' intrinsic learning motivation. If trainees enjoy the training, it might raise their interest in the topic and thus be an incentive for further learning. Our user study indicates that using a VPL can improve the learning experience, as participants found the learning process more enjoyable. Due to the promising results of the conducted user study, the potential of VPL usage for cybersecurity training appears encouraging. However, further experiments are necessary to validate our results' statistical significance and determine the training's effectiveness in terms of its long-term impact in the real-world context of an organization.

One aspect marginally tackled in this work is an approach to individually adapt the difficulty of tasks for each trainee. The user study showed that trainees might have different levels of knowledge and skill before engaging with the cyber range. Based on this, a variable *difficulty* could offer an optimal challenge for each trainee and thus yield a more significant learning outcome. Our refined approach suggested in this work allows the differentiation of the task difficulty. To decrease difficulty, all required attributes critical to solving the task could be automatically pre-arranged. Thereby, trainees only need to edit the values of these attributes. To increase difficulty, no attributes could be pre-arranged to display an empty header and rule block. Thus, trainees are required to first drag an attribute block into the head and rule block. Afterward, the editing of the values of the attributes remains. Based on the duration and number of mistakes in prior tasks, a dynamic number of blocks pre-arranged can be implemented.

Acknowledgment

This work is performed under the INSIST project, which is supported under contract by the Bavarian Ministry of Economic Affairs, Regional Development and Energy (DIK0338/01).

References

Bhatt et al., 2014. Bhatt, S., Manadhata, P. K., and Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*, 12(5):35–41.

Böhm et al., 2022. Böhm, F., Vielberth, M., and Pernul, G. (2022). Formalizing and integrating user knowledge into security analytics. *SN Computer Science*, 3(5):1–17.

Crowley and Filkins, 2022. Crowley, C. and Filkins, B. (2022). SANS 2022 SOC Survey. Technical report, SANS.

[6] https://github.com/BlocklyCyberRange/Refinement

Crumpler and Lewis, 2019. Crumpler, W. and Lewis, J. A. (2019). *The cybersecurity workforce gap*. Center for Strategic and International Studies (CSIS) Washington, DC, USA.

Davis and Magrath, 2013. Davis, J. and Magrath, S. (2013). A survey of cyber ranges and testbeds. Technical report, Defence Science and Technology Organisation Edinburg (Australia) Cyber and Electronic Warfare DIV.

Efklides, 2011. Efklides, A. (2011). Interactions of metacognition with motivation and affect in self-regulated learning: The MASRL model. *Educational psychologist*, 46(1):6–25.

Furnell et al., 2017. Furnell, S., Fischer, P., and Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, 2017(2):5–10.

Glas et al., 2022. Glas, M., Vielberth, M., Reittinger, T., Böhm, F., and Pernul, G. (2022). Visual programming in cyber range training to improve skill development. In Clarke, N. and Furnell, S., editors, *Human Aspects of Information Security and Assurance*, pages 3–13, Cham. Springer International Publishing.

Hart, 2006. Hart, S. G. (2006). NASA-task load index (NASA-TLX); 20 years later. In *Proceedings of the human factors and ergonomics society annual meeting*, volume 50, pages 904–908.

Hart and Staveland, 1988. Hart, S. G. and Staveland, L. E. (1988). Development of nasa-tlx (task load index): Results of empirical and theoretical research. In *Advances in psychology*, volume 52, pages 139–183. Elsevier.

Hwang and Helser, 2022. Hwang, M. I. and Helser, S. (2022). Cybersecurity educational games: a theoretical framework. *Information & Computer Security*, 30(2):225–242.

ISC², 2021. ISC² (2021). A Resilient Cybersecurity Profession Charts the Path Forward - ISC² Cybersecurity Workforce Study 2021. Technical report, International Information System Security Certification Consortium.

Kavallieratos et al., 2019. Kavallieratos, G., Katsikas, S. K., and Gkioulos, V. (2019). Towards a cyber-physical range. In *Proceedings of the 5th on Cyber-Physical System Security Workshop*, pages 25–34.

Keller, 1987. Keller, J. M. (1987). Development and use of the ARCS model of instructional design. *Journal of instructional development*, 10(3):2–10.

Lédeczi et al., 2019. Lédeczi, Á., Maróti, M., Zare, H., Yett, B., Hutchins, N., Broll, B., Völgyesi, P., Smith, M. B., Darrah, T., Metelko, M., et al. (2019). Teaching cybersecurity with networked robots. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, pages 885–891.

Lye and Koh, 2014. Lye, S. Y. and Koh, J. H. L. (2014). Review on teaching and learning of computational thinking through programming: What is next for K-12? *Computers in Human Behavior*, 41:51–61.

Nakata and Otsuka, 2021. Nakata, R. and Otsuka, A. (2021). Cyexec*: A high-performance container-based cyber range with scenario randomization. *IEEE Access*, 9:109095–109114.

National Initiative for Cybersecurity Education (NICE), 2020. National Initiative for Cybersecurity Education (NICE) (2020). The Cyber Range: A Guide. Technical report, National Initiative for Cybersecurity Education (NICE).

Newhouse et al., 2017. Newhouse, W., Keith, S., Scribner, B., and Witte, G. (2017). Cybersecurity Workforce Framework. Technical report, National Initiative for Cybersecurity Education (NICE).

Ouahbi et al., 2015. Ouahbi, I., Kaddari, F., Darhmaoui, H., Elachqar, A., and Lahmine, S. (2015). Learning basic programming concepts by creating games with scratch programming environment. *Procedia-Social and Behavioral Sciences*, 191:1479–1482.

Pawlicka et al., 2022. Pawlicka, A., Pawlicki, M., Kozik, R., and Choraś, M. (2022). Human-driven and human-centred cybersecurity: policy-making implications. *Transforming Government: People, Process and Policy*, 16(4):478–487.

Rao et al., 2018. Rao, A., Bihani, A., and Nair, M. (2018). Milo: A visual programming environment for Data Science Education. In *2018 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pages 211–215.

Schinagl et al., 2015. Schinagl, S., Schoon, K., and Paans, R. (2015). A framework for designing a security operations centre (soc). In *2015 48th Hawaii International Conference on System Sciences*, pages 2253–2262.

Schmutz et al., 2009. Schmutz, P., Heinz, S., Métrailler, Y., and Opwis, K. (2009). Cognitive load in eCommerce applications—measurement and effects on user satisfaction. *Advances in Human-Computer Interaction*, 2009.

Torgerson and Torgerson, 2001. Torgerson, C. J. and Torgerson, D. J. (2001). The need for randomised controlled trials in educational research. *British Journal of Educational Studies*, 49:316–328.

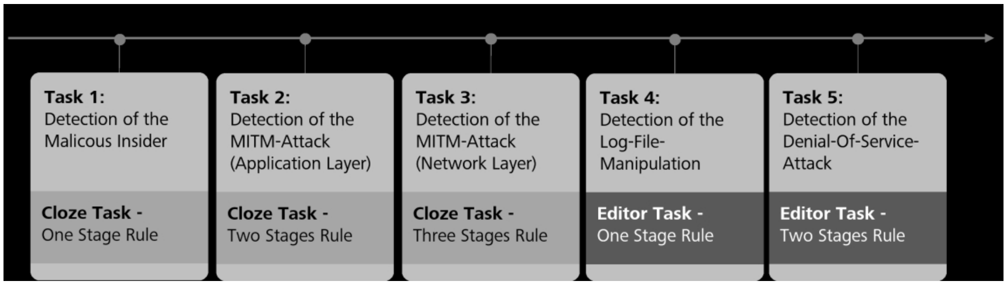
Tsai, 2019. Tsai, C.-Y. (2019). Improving students' understanding of basic programming concepts through visual programming language: The role of self-efficacy. *Computers in Human Behavior*, 95:224–232.

Vielberth et al., 2020. Vielberth, M., Bohm, F., Fichtinger, I., and Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, 8:227756–227779.

Vielberth et al., 2021. Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E., and Pernul, G. (2021). A Digital Twin-Based Cyber Range for SOC Analysts. In *Proc. of Data and Applications Security and Privacy XXXV - 35th Annual IFIP WG 11.3 Conference, DBSec 2021, Calgary, Canada*, pages 293–311. Springer International Publishing.

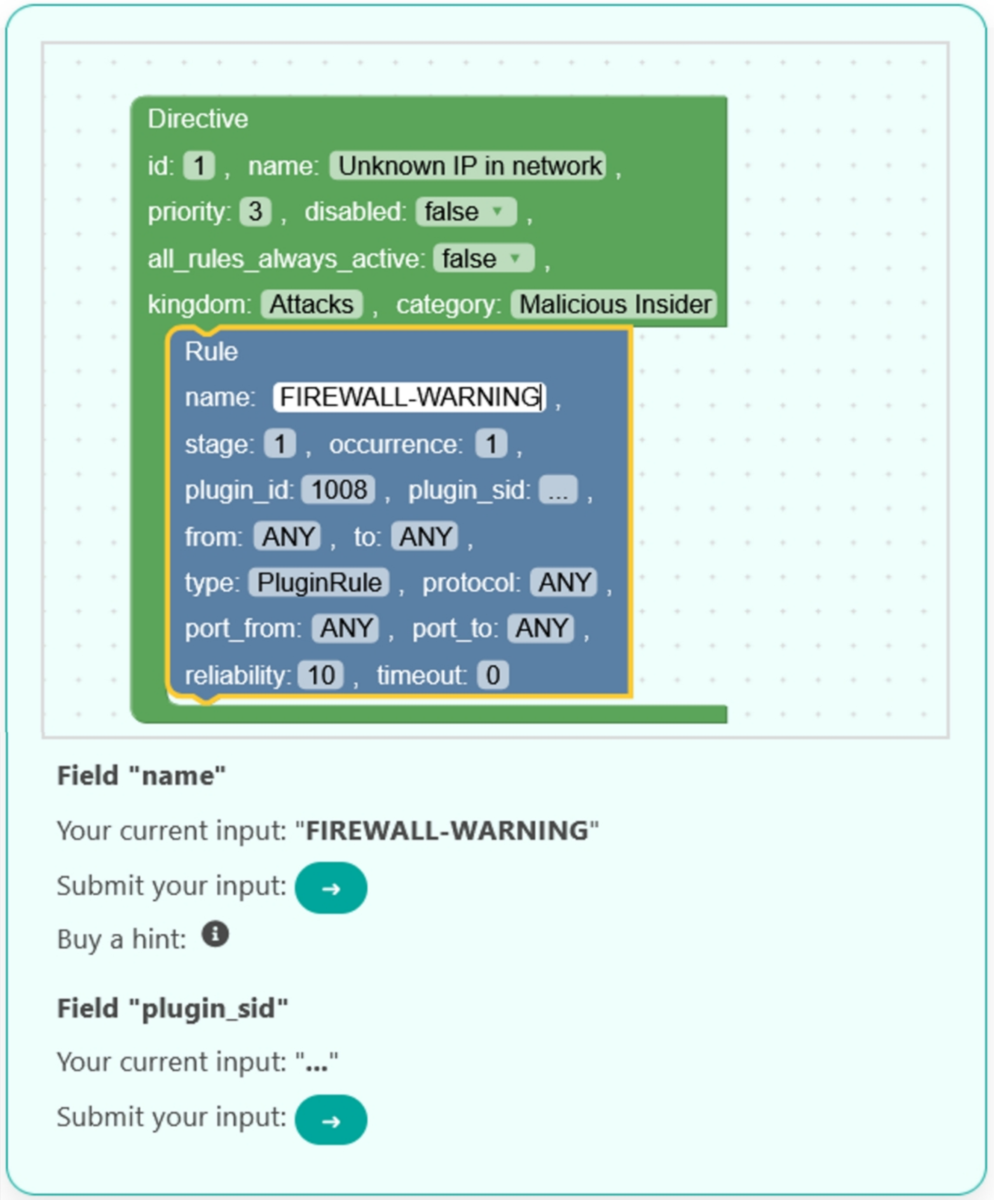
Vykopal et al., 2017. Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., and Tovarnak, D. (2017). Lessons learned from complex hands-on defence exercises in a cyber range. *Proceedings - Frontiers in Education Conference, FIE*, pages 1–8.

Yamin et al., 2020. Yamin, M. M., Katt, B., and Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636.


Task 1:
Detection of the Malicous Insider
Cloze Task -
One Stage Rule
Task 2:
Detection of the MITM-Attack (Application Layer)
Cloze Task -
Two Stages Rule
Task 3:
Detection of the MITM-Attack (Network Layer)
Cloze Task -
Three Stages Rule
Task 4:
Detection of the Log-File-Manipulation
Editor Task -
One Stage Rule
Task 5:
Detection of the Denial-Of-Service-Attack
Editor Task -
Two Stages Rule

Sequence of tasks in the cyber range training.

587x162mm (130 x 130 DPI)



Directive

id: 1 , name: Unknown IP in network ,

priority: 3 , disabled: false ,

all_rules_always_active: false ,

kingdom: Attacks , category: Malicious Insider

Rule

name: FIREWALL-WARNING ,

stage: 1 , occurrence: 1 ,

plugin_id: 1008 , plugin_sid: ... ,

from: ANY , to: ANY ,

type: PluginRule , protocol: ANY ,

port_from: ANY , port_to: ANY ,

reliability: 10 , timeout: 0

Field "name"

Your current input: "**FIREWALL-WARNING**"

Submit your input: →

Buy a hint:

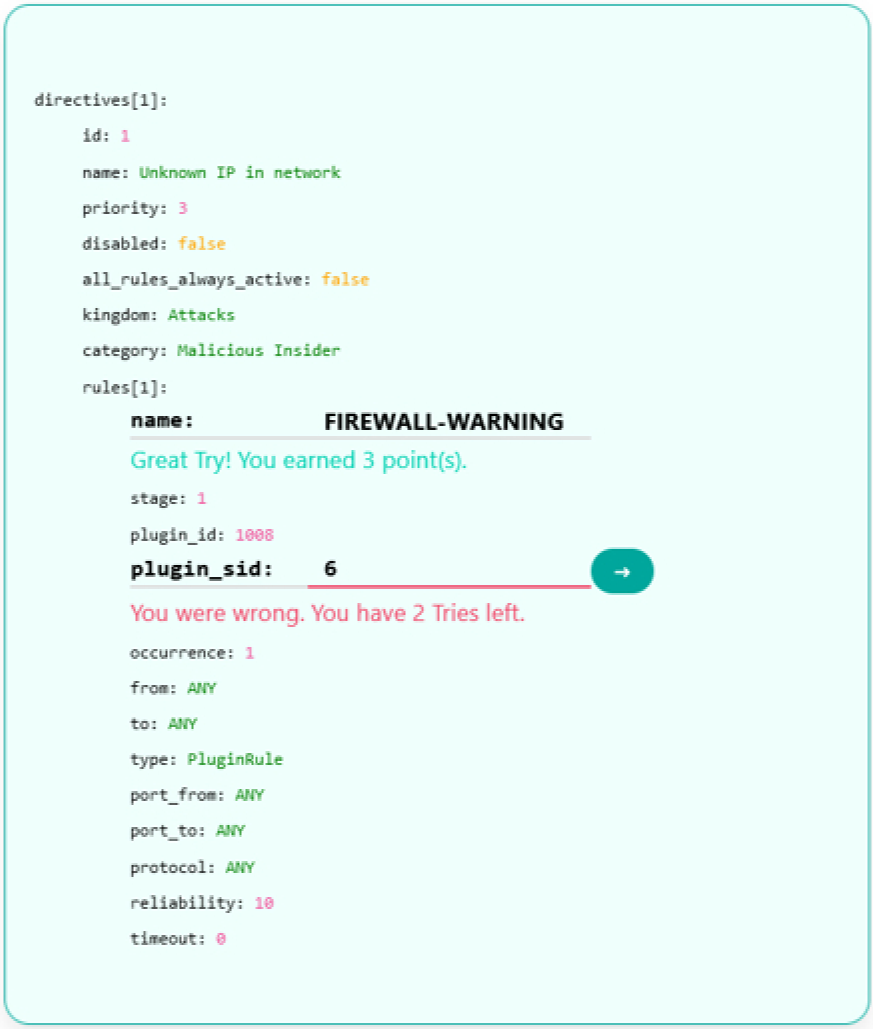
Field "plugin_sid"

Your current input: "**...**"

Submit your input: →

Comparison of a Cloze Task (Task 1) in Blocky and JSON mode - Blockly mode.

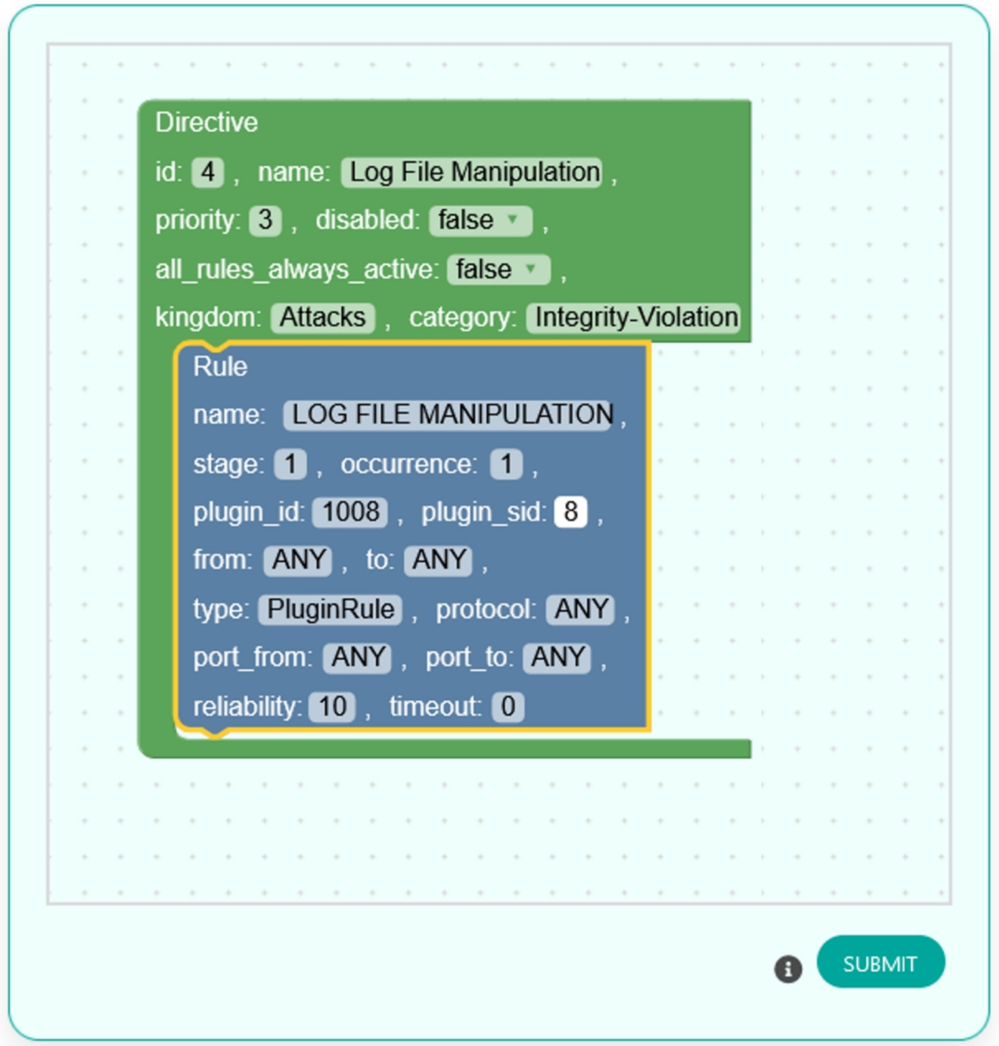
288x347mm (130 x 130 DPI)



```
directives[1]:
    id: 1
    name: Unknown IP in network
    priority: 3
    disabled: false
    all_rules_always_active: false
    kingdom: Attacks
    category: Malicious Insider
    rules[1]:
        name:        FIREWALL-WARNING
        Great Try! You earned 3 point(s).
        stage: 1
        plugin_id: 1008
        plugin_sid:  6
        You were wrong. You have 2 Tries left.
        occurrence: 1
        from: ANY
        to: ANY
        type: PluginRule
        port_from: ANY
        port_to: ANY
        protocol: ANY
        reliability: 10
        timeout: 0
```

Comparison of a Cloze Task (Task 1) in Blocky and JSON mode - JSON mode.

293x346mm (38 x 38 DPI)



Directive

id: 4 , name: Log File Manipulation ,

priority: 3 , disabled: false ,

all_rules_always_active: false ,

kingdom: Attacks , category: Integrity-Violation

Rule

name: LOG FILE MANIPULATION ,

stage: 1 , occurrence: 1 ,

plugin_id: 1008 , plugin_sid: 8 ,

from: ANY , to: ANY ,

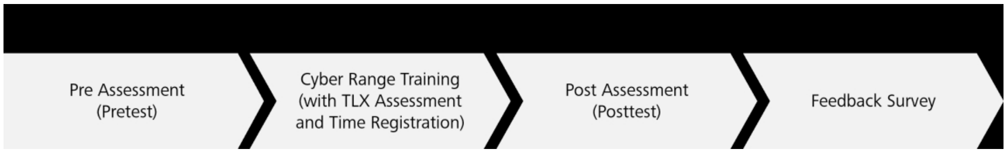
type: PluginRule , protocol: ANY ,

port_from: ANY , port_to: ANY ,

reliability: 10 , timeout: 0

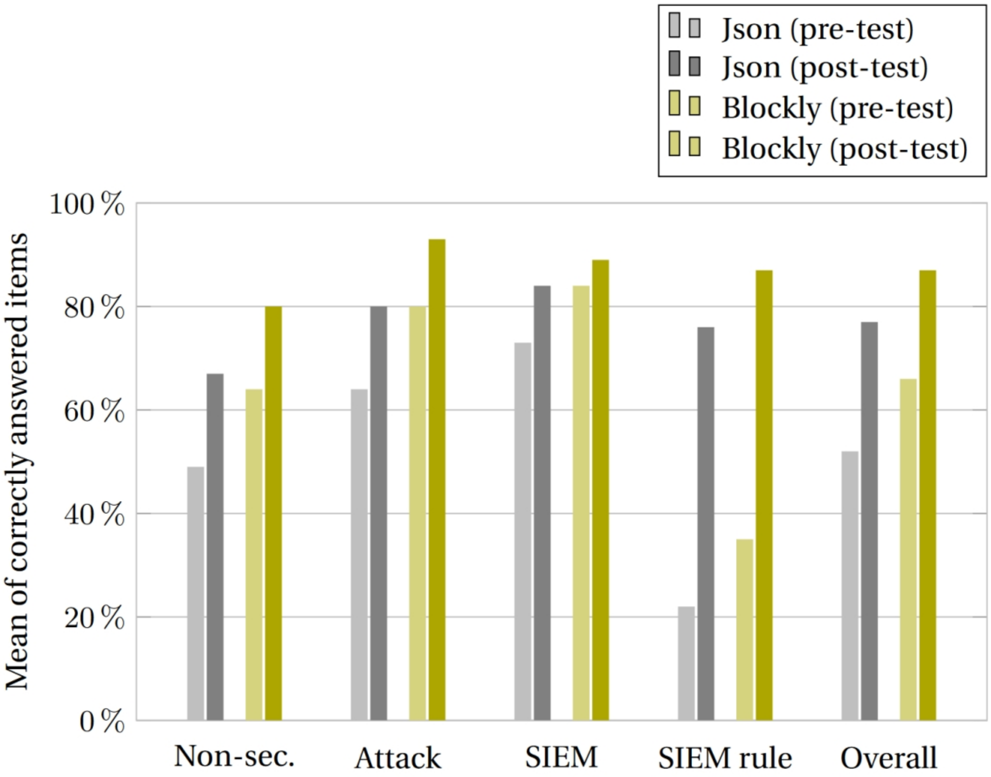
Comparison of a Editor Task (Task 1) in Blocky and JSON mode - Blockly mode.

286x302mm (130 x 130 DPI)


Pre Assessment (Pretest)
Cyber Range Training (with TLX Assessment and Time Registration)
Post Assessment (Posttest)
Feedback Survey

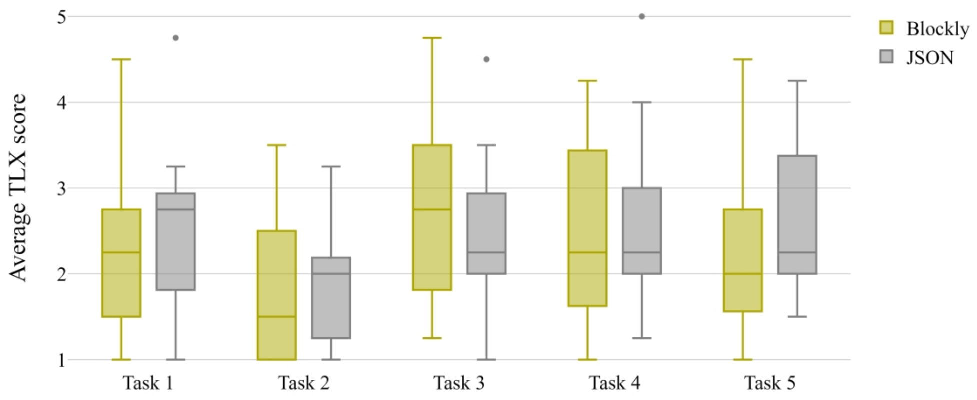
Procedure of the evaluation.

594x86mm (130 x 130 DPI)



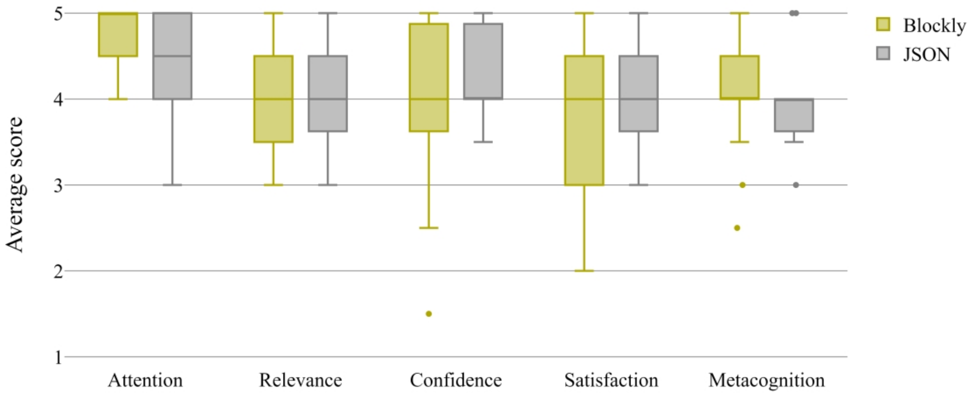
Graphical representation of learning outcome in both groups.

988x770mm (38 x 38 DPI)



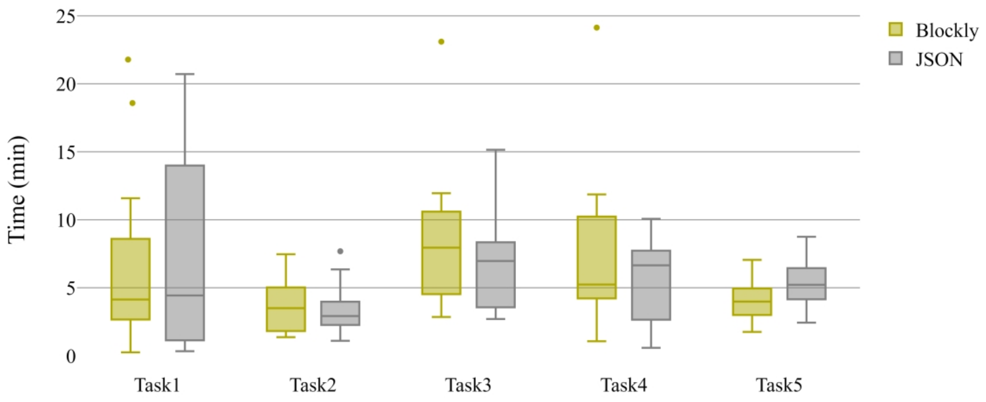
Graphical representation of H2 (learning experience) results: perceived workload based on TLX.

1411x705mm (72 x 72 DPI)



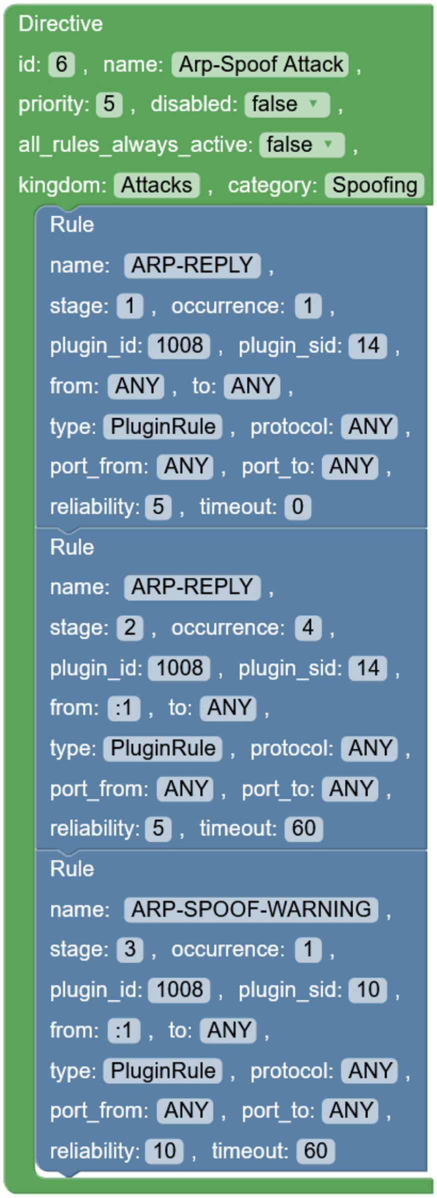
Graphical representation of H2 (learning experience) results: perceived workload based on ARCSM.

1411x705mm (72 x 72 DPI)



Graphical Representation of Learning Efficiency (H3) results.

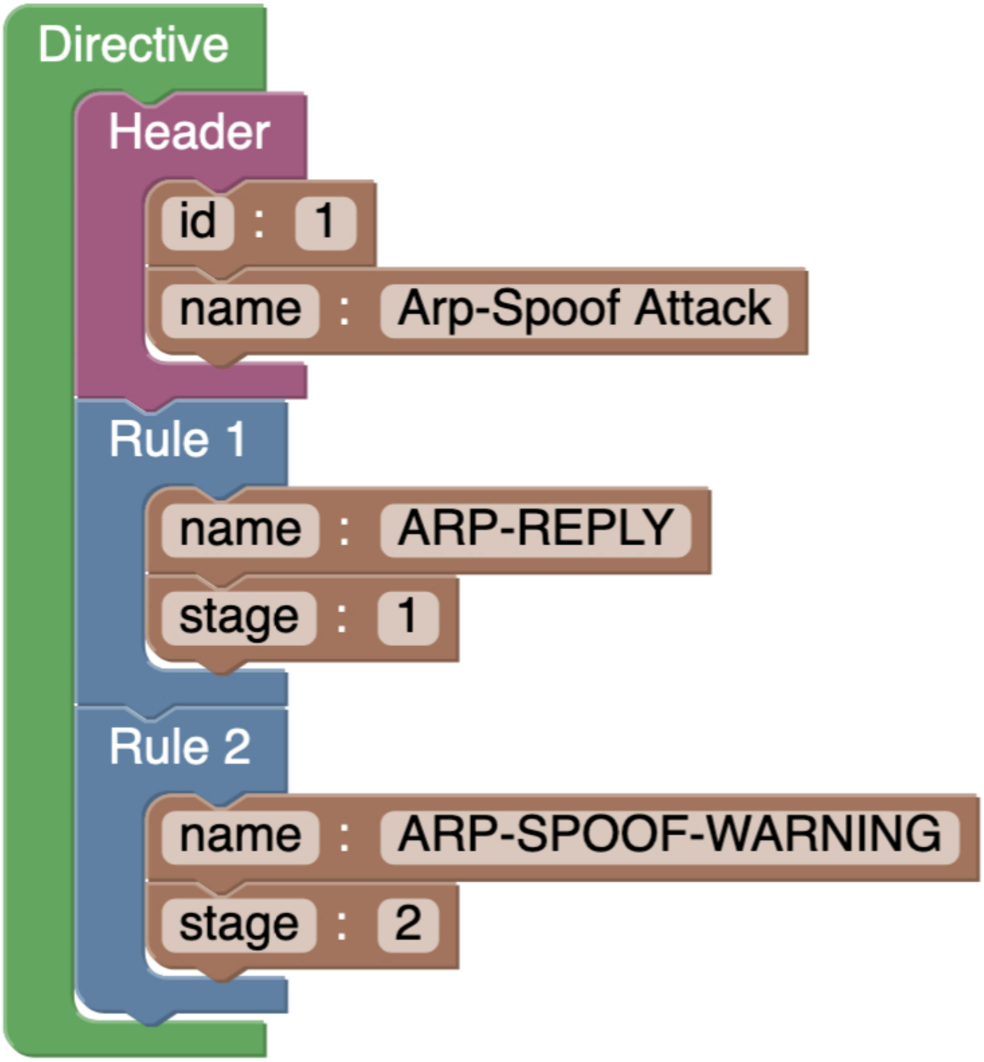
1411x705mm (72 x 72 DPI)



```
Directive
id: 6 , name: Arp-Spoof Attack ,
priority: 5 , disabled: false ▾ ,
all_rules_always_active: false ▾ ,
kingdom: Attacks , category: Spoofing
  Rule
  name: ARP-REPLY ,
  stage: 1 , occurrence: 1 ,
  plugin_id: 1008 , plugin_sid: 14 ,
  from: ANY , to: ANY ,
  type: PluginRule , protocol: ANY ,
  port_from: ANY , port_to: ANY ,
  reliability: 5 , timeout: 0
  Rule
  name: ARP-REPLY ,
  stage: 2 , occurrence: 4 ,
  plugin_id: 1008 , plugin_sid: 14 ,
  from: :1 , to: ANY ,
  type: PluginRule , protocol: ANY ,
  port_from: ANY , port_to: ANY ,
  reliability: 5 , timeout: 60
  Rule
  name: ARP-SPOOF-WARNING ,
  stage: 3 , occurrence: 1 ,
  plugin_id: 1008 , plugin_sid: 10 ,
  from: :1 , to: ANY ,
  type: PluginRule , protocol: ANY ,
  port_from: ANY , port_to: ANY ,
  reliability: 10 , timeout: 60
```

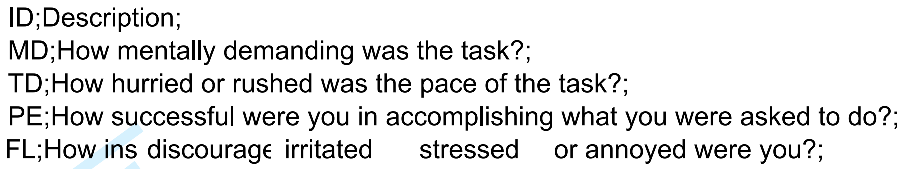
Extant prototype.

276x751mm (38 x 38 DPI)



Refinement prototype.

262x281mm (72 x 72 DPI)



ID;Description;
MD;How mentally demanding was the task?;
TD;How hurried or rushed was the pace of the task?;
PE;How successful were you in accomplishing what you were asked to do?;
FL;How ins discourage irritated stressed or annoyed were you?;

ID;Description
A1;The scenario and context of the training were interesting.
A2;I wanted to successfully finish the training and complete all the tasks.

```
Group;Category;M (Pre);SD (Pre);M (Post);SD (Post);t;df;Sig (2-tailed)
Blockly;Non-sec.-related;0.64;0.29;0.8;0.21;-1.83;14;0.089
;Attack-related;0.8;0.17;0.93;0.14;-3.06;14;0.009
;SIEM-related;0.84;0.21;0.89;0.16;-1;14;0.334
;SIEM rule-related;0.35;0.39;0.87;0.25;-4.08;14;0.001
;Overall;0.66;0.15;0.87;0.1;-5.43;14;<.001
JSON;Non-sec.-related;0.49;0.21;0.67;0.18;-2.48;14;0.027
;Attack-related;0.64;0.27;0.8;0.21;-2.17;14;0.048
;SIEM-related;0.73;0.26;0.84;0.21;-1.43;14;0.173
;SIEM rule-related;0.22;0.21;0.76;0.29;-6.29;14;<.001
;Overall;0.52;0.13;0.77;0.17;-4.61;14;<.001
;;;;;;;;
```

Category	M (Blockly)	SD (Blockly)	M (JSON)	SD (JSON)	t	df	Sig (2-tailed)
Non-sec.-related	0.16	0.33	0.18	0.28	-0.20	27.21	0.84
Attack-related	0.13	0.17	0.16	0.28	0.27	23.11	0.79
SIEM-related	0.04	0.17	0.11	0.30	-0.75	22.32	0.46
SIEM rule-related	0.51	0.49	0.53	0.33	-0.15	24.59	0.89
Overall	0.21	0.15	0.24	0.21	-0.51	25.69	0.62

```
Task;M (Blockly);SD (Blockly);M (JSON);SD (JSON);t;df;Sig. (2-tailed)
Task 1;2.25;0.93;2.53;0.9;-0.85;27.97;0.404
Task 2;1.78;0.83;1.88;0.68;-0.36;26.98;0.721
Task 3;2.67;1.06;2.45;0.91;0.6;27.36;0.552
Task 4;2.57;1.06;2.58;0.98;-0.04;27.8;0.965
Task 5;2.35;1.01;2.62;0.85;-0.78;27.24;0.442
```

Condition	M (Blockly)	SD (Blockly)	M (JSON)	SD (JSON)	t	df	Sig (2-tailed)
Attention	4.67	0.41	4.43	0.65	1.18	23.54	0.251
Relevance	4.03	0.55	4.07	0.56	-0.16	27.99	0.871
Confidence	4	0.98	4.3	0.53	-1.04	21.47	0.309
Satisfaction	3.67	0.96	4	0.57	-1.16	22.74	0.258
Metacognition	4.1	0.71	3.97	0.52	0.59	25.53	0.562

```
Task;M (Blockly);SD (Blockly);M (JSON);SD (JSON);t;df;Sig (2-tailed)
Task 1;06:38;06:19;07:07;06:53;-0.2;27.89;0.844
Task 2;03:41;02:12;03:21;01:44;0.45;26.56;0.654
Task 3;08:37;04:59;06:39;03:29;1.25;15.07;0.223
Task 4;07:27;05:37;05:21;03:12;1.26;22.2;0.22
Task 5;04:11;01:25;05:11;01:44;-1.75;26.98;0.091
```